Content

Last updated: 08/04/26

1. INTRODUCTION

HeliosX Group and its subsidiaries, MedExpress Enterprises Ltd, MedExpress Pharma EU Ltd, Apotheek Blauwe B.V., Central Medical Solutions Ltd, Dermatica Ltd, Avianta Holdings Ltd, Avianta Pharma Ltd and Avianta Pharma EU Ltd are committed to ensuring full compliance with all Data Protection (DP) and Information Governance (IG) related laws, legislation, guidance, regulatory and contractual requirements in relation to DP & IG thereof.

This Privacy Notice describes our policies and procedures on the collection, use and disclosure of your information when during and after the recruitment process. It applies to anyone who is applying to work for us, whether as an employee, worker, apprentices, interns, agency workers and directors (‘’You’’).

It also outlines your Information Rights and how the law protects you.

Please note that we will not necessarily hold, use or share all of the types of personal data described in this Privacy Notice in relation to you. The specific types of data about you that we will hold, use and share will depend on the role for which you are applying, the nature of the recruitment process, how far you progress in the recruitment process and your individual circumstances.

We are required by data protection law to give you the information in this Privacy Notice. It is important that you read the Privacy Notice carefully, together with any other similar or additional information that we might give you from time to time about how we collect and use your personal data.

Should your application be successful, when you start work for us, we will provide you with another privacy notice that explains how we deal with your personal data whilst you are working for us.

We take our responsibilities in relation to data protection and information rights seriously and maintain robust processes for safeguarding the personal information we hold in order to carry out our services and provide easy access to the information rights of individuals.

2. PURPOSE

You are being provided a copy of this privacy notice because you are applying for work with us in one of the capacities outlined above. This notice makes you aware of how and why your personal data will be used, namely for the purposes of the recruitment exercise, and how long it will usually be retained for. It provides you with certain information that must be provided under the UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018 (“DPA”). If applicable, we may also process your data under the EU General Data Protection Regulation (EU GDPR) when handling applications from the European Economic Area (EEA). The purpose of this notice is to provide you with clear information about how

your personal data is processed by HeliosX Group and its subsidiaries, the lawful basis for processing, and your rights under data protection laws. We are committed to ensuring that recruitment personal data is handled lawfully, fairly, and transparently.

3. SCOPE

This Privacy Notice applies to anyone who is applying to work for HeliosX Group and its subsidiaries, listed above.These companies may process or provide personal data in the course of their recruitment.

This notice covers personal data collected during recruitment, employment, and post-employment activities.

4. DEFINITIONS

Key terms used within this policy are defined in the glossary (Appendix 1)

5. RESPONSIBILITIES

HeliosX Group acts as the data controller in relation to personal data and ensures compliance with data protection laws.

We will comply with data protection law and principles, which means that your data will be:

- Used lawfully, fairly and in a transparent way.
- Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
- Relevant to the purposes we have told you about and limited only to those purposes.
- Accurate and kept up to date.
- Kept only as long as necessary for the purposes we have told you about.
- Kept securely.

HeliosX Group's Data Protection Officer (DPO) oversees data protection compliance, provides guidance, and acts as a point of contact for data subjects.

6. POLICY

What type of ordinary personal data do we hold about you and why?
At the initial stages of recruitment, we collect, hold and use the following types of ordinary personal data about you:

Information We Collect from You

- Information contained in your application form/CV/covering letter, including, but not limited to, basic personal details such as your name, title, contact details (including email and postal addresses and mobile phone number), preferred method of contact, photograph, if provided, employment history, experience, skills, qualifications/training

(including educational, vocational, driving licences where appropriate), referees' names and contact details, etc.

- Selection information, including correspondence, interview notes, internal notes, the results of any written or online selection tests
- Availability and work eligibility details including but not limited to your notice period, preferred start date, current and/or future work eligibility status, visa type, and visa expiry date.
- Documents you provide throughout the application process including but not limited to CVs, covering letters, and assessment outputs. These documents may contain information on your employment history, academic qualifications/history, professional training/certifications, skills, and experiences.
- Application details including but not limited to the source of your application, the date/time, the role(s) you applied for, salary history/expectations, and Equal Opportunities statements.
- Records of electronic communications, including but not limited to the content and attachments of emails.

Information We Collect/Generate About You

- Publicly available data including but not limited to your professional social networks (primarily LinkedIn, but also GitHub, Stack Overflow, and similar networks.).
- Job application progress including but not limited to the stages you complete of the recruitment process, records of interviews, interview notes/feedback, assessment feedback, rejection stage/s, rejection reason/s, and job offer details.

If you receive a conditional offer of employment, we may collect, hold and use the following additional types of ordinary personal data about you:

- Pre-employment check information, including references and verification of qualifications.
- Right to work checks and related documents including passport or similar ID documents containing date and place of birth, amongst other information.
- Pre-employment screening.

We hold and use this personal data so that we can:

- Process your application and correspond with you in relation to the/any recruitment process/es.
- Consider your application in relation to the role for which you have applied, including assessing whether you have the required skills, experience, qualifications and training for a role within the company.
- Consider your application in relation to other roles at HeliosX Holdings and subsidiary companies, both at present and in the future (see How Long We Keep Your Personal Data below for more information on our data retention policy).
- Make informed recruitment decisions.
- Verify information provided by you.
- Conduct and report on criminal history as part of the background check process.
- Check and demonstrate that you have the legal right to work in the UK.
- Keep appropriate records of our recruitment process and decisions.
- Enhance any information that we receive from you with information collected, generated, or obtained throughout our recruitment processes, including interview

scorecards and feedback, assessment outcomes, internal evaluation notes, stage progression and hiring decisions. In some cases we may also review publicly available professional information. This information is collected to enable structured candidate evaluation, support hiring decisions and maintain records of the recruitment process.
- Help HeliosX Holdings and subsidiary companies improve the effectiveness and efficiency of our recruitment systems and processes.

Please contact us at talent-operations@heliosx.com should you have any questions or would like to request additional information regarding any aspect of our checks, including criminal history and background checks. All personal data provided, collected, generated, or obtained will be processed through Greenhouse Software Inc., a recruitment platform provider located in the United States of America (USA), engaged by us to help manage our recruitment and hiring processes. Accordingly, your personal data will be transferred to, and stored, in the USA. In addition to Greenhouse, we may also receive candidate applications via external job boards and sourcing platforms such as Otta, Indeed and LinkedIn. In these cases, candidate data (e.g. CV, name and contact details) may initially be processed by those platforms before being transferred into Greenhouse as part of the recruitment process. The Google Suite and Gemini are used as standard operational tools to facilitate interviews and interview transcription. Transfers to Greenhouse and, where applicable, the above job boards and platforms, in the United States are safeguarded using Standard Contractual Clauses approved by the UK Information Commissioner's Office, along with supplementary measures as needed to ensure your data is protected in accordance with UK data protection law.

For right to work checks and referencing we use a UK-based platform called Zinc.

We take appropriate measures to ensure that all personal data is kept secure, including security measures to prevent personal data from being accidentally lost, used, or accessed in an unauthorised way. Within HeliosX Holdings and subsidiary companies, we limit access to your personal data to those who have a genuine need to access it: the People/Talent Team, the Hiring Manager for the role in question, interviewers/assessment reviewers for the role in question. In particular situations, or for specific roles, the data may also be shared with the Executive Board, and the Director responsible for the department associated with the role (note that there may be overlap and variation between the people in those positions and involved in the process). Overall, those processing your personal data will do so only in an authorised manner, and are subject to a duty of confidentiality.

We have procedures in place to deal with any suspected data security breach. We will notify you and any applicable regulator of a suspected data security breach where we are legally required to do so.

What is our lawful basis for processing your personal data?
Data protection law specifies the legal grounds on which we can hold and use personal data. We rely on one or more of the following lawful basis when we process your ordinary personal data:

- We need it to take steps at your request, such as confirming your identity, in order to enter into a contract of, or for, employment or services with you.

- We need it to comply with a legal obligation, e.g. the obligation not to discriminate during our recruitment process, or the obligation not to employ someone who does not have the legal right to work in the UK.
- It is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests. For example, it is in our legitimate interests to review and consider your personal data (as listed above) so that we can select the most appropriate candidate for the job.

What type of special category personal data do we hold about you, why, and on what legal grounds?

Where we collect special category data, such as information about your ethnicity, health, or disability status for equal opportunities monitoring, we will only do so with your explicit consent and for the purposes of complying with our legal obligations.

We will only collect, hold and use limited types of special category data about you during the recruitment process, as described below. Since special category data is usually more sensitive than ordinary personal data, we need to have an additional legal ground (as well as the legal grounds set out in the section on ordinary personal data, above) to collect, hold and use it. The additional legal grounds that we rely on to collect, hold and use your special category data are explained below for each type of special category data.

At the initial stages of recruitment, we collect, hold and use the following special category data about you:-

Equal opportunities monitoring
Equal opportunities monitoring data which could include information about your race or ethnicity, religious beliefs, sexual orientation or health. We use this information to monitor equality of opportunity and diversity in our recruitment process. Our additional legal ground for using this information is that it is necessary in the public interest for the purposes of equal opportunities monitoring and is in line with our Data Protection Policy.

Adjustments for disability/medical conditions
Information relevant to any request by you for adjustments to the recruitment process as a result of an underlying medical condition or disability. We use this information to enable us to carry out a fair, non-discriminatory recruitment process by considering/making reasonable adjustments to our process as appropriate. Our additional legal ground for using this information is that we need it to comply with a legal obligation/exercise a legal right in relation to employment – namely, the obligations not to discriminate, and to make reasonable adjustments to accommodate a disability – and such use is in line with our Data Protection Policy.

If you are shortlisted for a position, or you receive a conditional offer of employment, we may collect, hold and use the following additional types of special category personal data about you:
Pre-employment health questionnaires/medicals

We collect information about your health in a pre-employment medical questionnaire and/or examination, as well as any information about underlying medical conditions and adjustments that you have brought to our attention. We use this information to assess whether you are fit to do the job with adjustments, to consider/arrange suitable adjustments and to comply with health and safety requirements. Our additional legal grounds for using this information are that: we need it to comply with a legal obligation/exercise a legal right in relation to employment – namely, the obligation to make reasonable adjustments to accommodate a disability – and such use is in line with our Data Protection Policy; and it is needed to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards.

How do we collect your personal data?
You provide us with most of the personal data about you that we hold and use, for example information you provide on application forms, in email and telephone conversations with our representatives, and in job interviews and assessments.Some of the personal data we hold and use about you is generated from internal sources during the recruitment process such as information we generate following your interactions with our staff, systems, and processes. For example, the person interviewing you may score your suitability for the role, and we record the reasons for decisions made about whether or not your application is successful.

Some of the personal data about you that we hold, and use may come from external or publicly available sources online. For example, a third party such as a recruitment agency provides us with a shortlist of candidates, or via referrals or references. If we offer you a role, we will carry out pre-employment checks, such as taking up references from past employers or education providers and we may check your qualifications by contacting the awarding body. (References are only sought with your express prior permission, and typically happen at the point of offer). We may ask an occupational health professional to report to us on your fitness to do the job. We may seek a criminal record check from the DBS. In some circumstances, we may ask the Home Office for information about your immigration status to verify your right to work in the UK. For some roles, we may also obtain information about you from publicly available sources, such as your LinkedIn profile or other media sources.

Who do we share your personal data with?
We may disclose personal data to third parties under certain circumstances. Before doing so, we will assess the lawfulness (including necessity and proportionality) of the disclosure. Such third parties may include:

- Other members of our group, specifically any senior management for the business unit and for the group company that is relevant in order to make decisions around hiring and remuneration.
- Trusted service providers such as IT service providers which assist with the hosting and maintenance of our websites and digital infrastructure and background check providers.
- Third parties who are part of the administrative and management structure of the entity you are applying to;
- Regulatory authorities, courts, tribunals, and governmental agencies; and

- Enforcement agencies such as police and debt collecting agencies.

Personal data can also be shared to a third party if:

- Where we have been instructed to do so by law
- Where we believe the reasons for sharing are so important, they override our obligation of confidentiality. Such as to support the investigation and prosecution of offenders or to prevent serious crime.
- Where we are legally required to do so.

How long do we keep your personal data for?

We will keep your personal data throughout the recruitment process.

If your application is successful, when you start work for us you will be issued with an Employee Privacy Notice which will include information about what personal data we keep from the recruitment process and how long we keep your personal data whilst you are working for us and after you have left.

If your application is unsuccessful, we will retain your personal information for a period of 12 months from the date we notify you of our decision.

We retain your personal information for that period so that we can show, in the event of a legal claim, that we have not discriminated against candidates on prohibited grounds and that we have conducted the recruitment process in a fair and transparent way. After this period, we will anonymise and retain your personal information in accordance with our data retention policy.

If we would like to retain your personal information on file, on the basis that we might be able to consider you for an opportunity that may arise in future, we will write to you separately, seeking your explicit consent to retain your personal information for a fixed period usually 12 months, for that purpose. At the end of the agreed timeframe, we will anonymise the data.

In all cases, we will not keep your personal data for longer than we need it for our legitimate purposes.

What are your rights in relation to your personal data?

Under the Data Protection Act 2018 you have certain legal rights in relation to how your personal data is processed. These are:

- **Right of Access** (We have to tell you if we have your personal data, what it is used for and let you have access if you request it, which is known as a Subject Access Request).
- **Right to Rectify** (We can correct your personal data if you request us to).
- **Right of Erasure** (If we do not have a lawful basis for holding your information, for instance we are relying on your consent and you withdraw that consent, then we have to delete your personal data).
- **Right to Restriction** (If you want us to stop processing your personal data but do not want it deleted).

- **Right of Portability** (If you request us to transfer your personal data in a common, machine-readable format to another organisation).
- **Right to Object/Restrict Processing** (If you want us to stop processing your personal data but do not want or cannot have it deleted).

Under Data Protection law, you have the Right of Access to the personal data that we have collected and processed about you. This right includes both the right to know if we have collected personal data on you and also the right to see what personal data we have collected.

If you would like to exercise any of the above rights, please contact us at: talent-operations@heliosx.com.

Your right to log a complaint with the supervisory authority
We hope that we can resolve any query or concern you raise about our use or processing of your personal data. If you are not satisfied with our processes or approach we would request that you please contact us first.

The UK GDPR gives you the right to file a complaint with a supervisory authority. In the UK, this is the Information Commissioner's Office (ICO), while the EU GDPR gives you the right to file a complaint with the relevant supervisory authority in the European Union (or European Economic Area) state where you work, live, or where any alleged infringement of data protection laws occurred. In the UK, the ICO may be contacted at http://ico.org.uk/concerns/ or on 0303 123 1113.

7. MONITORING AND COMPLIANCE

HeliosX Group regularly reviews and updates data protection policies and practices.
We may amend this Privacy Notice at any time. Any changes we may make will be posted on this page, so please check back frequently. Your continued use of our website and our services after posting will constitute your acceptance of, and agreement to, any changes.

8. APPENDICES

Appendix One – Terms and Definitions

Term	Definition
Privacy Notices	A public document which explains how that organisation processes personal data and how it applies data protection principles.

Special Category Data	Special category data refers to data which reveals: "Racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purposes of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation".
Data Controller	The person or organisation that determines when, why and how to process personal data. It is responsible for establishing practices and policies in accordance with data protection law. HeliosX is the Data Controller of all personal data relating to it.
Data Processor	Any natural or legal person, public authority, agency, or other body which processes data on behalf of the controller.
Data Processing	Any activity that involves the use of personal data. It includes obtaining, recording, or holding the data or carrying out any operation or set of operations on the data, including organising, amending, retrieving, using, disclosing, erasing, or destroying it. Processing also includes transmitting or transferring Personal Data to third parties. In brief, it is anything that can be done to personal data from its creation to its destruction, including both creation and destruction.
Data Protection Officer (DPO)	An internal or externally assigned independent expert who assists organisations in monitoring internal compliance, informing and advising on data protection obligations, advising on Data Protection Impact Assessments (DPIAs), and acting as a point of contact for data subjects and the Information Commissioner's Office (ICO).
Data Subject	Any individual person who can be identified, directly or indirectly, via an identifier such as a name, an ID number, location data, or via factors specific to the person's physical, physiological, genetic, mental, economic, cultural, or social identity.
Information Commissioner's Office (ICO)	Independent regulatory body in the United Kingdom that is responsible for promoting and enforcing data protection and privacy laws.
UK Data Protection Act 2018 (UK GDPR)	Is a law that governs the processing of personal data in the United Kingdom. The Data Protection Act 2018 applies to the processing of personal data that is performed automatically, or as part of a structured filing system, as well as to the processing of manual records that are intended to form part of such a system.
EU GDPR	The European Data Protection Regulation is applicable as of May 25, 2108, in all member states to harmonise data privacy laws across Europe. Although it no longer applies to

	the processing of UK personal information, it still applies to UK organisations that process EU residents' personal data.